



ÆGIS journal

Addressing threats that affect your bottom line

Volume 10 Number 4, April 2007

From the case files of

LUBRINCO

<http://www.lubrinco.com/>

and

FE&E CLARITY FROM COMPLEXITY
Financial Examinations & Evaluations, Inc.

<http://www.feeinc.com/>

Intellectual property being stolen or at risk? Call us!

This month's features:

- **Special Announcements: IPCI Conference moved to 2-3 October 2007**
- 1. **Asset Location and Due Diligence — Whom do you trust?**
- 2. **OPSEC, Economic Espionage, and Competitive Intelligence — IP fraud**
- 3. **Executive Protection — آٹا گيلا هونا غريبي ميں**
- 4. **Technical Issues — Who should investigate your fraud?**
- 5. **Real Stories from the Field — How dead is dead?**
- 6. **Book and Product Reviews — Centerpoint Awakening Prologue**
- 7. **Subscription/Unsubscription/Copyright Information**



PLEASE NOTE THAT BECAUSE OF LOGISTICAL PROBLEMS THE CONFERENCE HAS BEEN RE-SCHEDULED.

AEGIS journal, in conjunction with
The Center for the Study of Law, Science, and Technology,
Sandra Day O'Connor College of Law at Arizona State University
and
The OPSEC Professionals Society
will be hosting its two-day **Critical Information and IP Conference:**
Identification, Valuation, and Protection of Critical Information and Intellectual Property
For Directors, Finance Officers, and Counsel
At Arizona State University in Tempe, Arizona, **2-3 October 2007**
For information, contact us at conference@aegisjournal.com

L. Burke Files will be moderating a panel on “Understanding Offshore Insurance” at the
Fifth annual Offshore Alert Financial Due Diligence Conference
24-25 April 2007 Miami, Florida <http://www.offshorealert.com/>

1. Asset Location and Due Diligence — Whom do you trust?

Two of the editors of this journal recently spoke to a group of bankers and journalists in Tashkent on Anti-Money Laundering, Fraud, as well as Identification, Valuation, and Protection of Critical Information/Intellectual Property.

One of the bankers commented that before giving a loan they would go out to see the enterprise, view the equipment, and interview the applicant. On several occasions, however, after the loan had been made, the people and the machinery would disappear. What were they doing wrong?

The answer was that they were interviewing the wrong people. Rather than

devoting all their time to the applicants, they needed to be dealing with the secondary characters, such as the neighbors. The neighbors would be able to tell them that the people and equipment had recently arrived, and had no history in the area. Similarly, the ownership of the equipment needed to be verified. Heavy equipment that was rented for a week was not an indication of an ongoing enterprise. An ancillary benefit is that when this approach is taken, more people (the neighbors) are aware of the bank, and the care and interest in which they treat their customers.

The more money that is involved, the further afield we tend to go in doing background checks. The job of the due diligence investigator is to determine what is true about the application and what is not. This includes checking out the *bonafides* of the applicant, including assuring that they are who they say they are, and not merely that they have documents saying who they are; and that the circumstances that they describe are the actual circumstances, and not an elaborate net of lies.

Banks make money by collecting on the loans, and they make money by making good loans, not bad loans. Most applicants are relatively honest, and don't require an inordinate amount of investigation. The bigger the amount of money involved, the more care that needs to go into it. Even on smaller projects you need to develop some sense of when things look right, and when something just seems wrong.

2. OPSEC, Economic Espionage, and Competitive Intelligence — IP fraud

We see more financial fraud every week than most companies see in a year. We deal with more financial fraud in a month than most government agencies are likely to encounter in a decade. Because of this, we spend a lot of time thinking about financial fraud: It is our business. We are also heavily involved in the identification, valuation, and protection of critical information and intellectual property.

When looking at loss of intellectual property and critical information we must distinguish among two types of information. The first is that which is publicly available in the form of copyrighted material, trade and service marks, and patents. Misuse of these is dealt with by attorneys and accountants, with some security measures, like generally-ineffective copy

protection on CDs and DVDs. There are a host of competent companies that provide expertise in this area of intellectual property.

The second is information that you would prefer not to be public. This would include trade secrets, proprietary processes, customer lists, sales figures, marketing plans, travel plans, and a host of other information. This class of information is of benefit to a company in part because it is not known to competitors and adversaries. Losses in this area come from competitive intelligence, economic espionage, theft, plus from simply giving the information to your competitors and adversaries. These losses are dealt with via counter-intelligence, which is an area in which neither your attorneys, nor your accountants, nor your consultants are likely to have training and expertise. Counter-intelligence is LUBRINCO's area of specialty, and there are only a handful of private-sector companies playing in this ball park.

Like most, we thought of financial fraud and loss of critical information and intellectual property as two different things. Of late, however, because we are so active in both fields, it has become clear to us that loss of money because intellectual property has been compromised falls into the category of fraud. Unfortunately, the terms we use in describing fraud, and the way we think of both fraud and intellectual property, don't quite fit reality. They are parallel universes, if you will.

For a start, financial fraud is a zero-sum game: What the fraudster takes you no longer have. With loss of intellectual property, however, the game changes substantially. What you have lost is not the IP itself, but, rather, the *exclusivity* of access to your intellectual property.

In a 19th and 20th century view of economics, this did not seem important, because the focus was on things and money. Thus, if you speak with the PCAOB about accounting for intellectual property, you will discover something that your accountants already know: Intellectual property developed in-house has no book value. It is magically folded into goodwill.

In the late 20th and early 21st centuries, intellectual property grew rapidly, and now represent over 70% of the value of a modern business entity. And yet, this intellectual property still has no book value! Thus, while IP fraud is estimated – in our opinion under-estimated – to have reached half the value

of traditional financial fraud, it all involves loss of something that has no book value.

In addition, many of the techniques set by CPAs to facilitate your bookkeepers and accountants in dealing with financial fraud are not responsive when dealing with intellectual property fraud. Intellectual property fraud requires the implementation of an OPSEC program by an OCP. (The OPSEC Certified Professional is the IP equivalent of a CPA.) This creates a set of expertise barriers. Your CPA and counsel can help you deal with financial fraud, but you need an OCP to deal with IP fraud, and you probably don't have one on your staff. You don't even have an OAP (OPSEC Associate Professional, one step below the OCP) to help run the program designed by the OCP.

The good news is that the SEC recognizes the importance of tracking losses from fraud, and has said this specifically includes losses caused by economic espionage and information theft, which, by definition, includes losses to competitive intelligence. The bad news is that most companies are not yet equipped to deal with IP fraud.

This will change once there is a shareholder suit in which senior managers and directors are found to be personally liable, with this liability being uncovered by D&O policies.

3. Executive Protection — آٹا گيلا ہونا غريبي ميں

When someone does something wrong, they often don't want to admit it. This is not unnatural, as few people wish to suffer if they can avoid it. There are three general categories that determine one's willingness to take responsibility for one's choice of actions.

- The first is ethical: You simply don't want to do things that you consider to be wrong, and may well 'fess up to it, independent of the consequences.
- The second is moral: You fear punishment in the hereafter more than you desire temporal benefit.
- The third is a dollars-and-cents evaluation that says it will cost you less now than if you pretend the product isn't defective and have to pay later.

Unfortunately, not everyone is an Eagle Scout. And many religious people are able to interpret the scripture of their choice in such a way as to justify bad actions. And sometimes the cost analysis may tell you to do the wrong thing if you believe that the end justifies the means, an ethical view that distorts most ethical ideas. In addition, there are many people who are simply criminals, for whom issues of right and wrong do not apply, and where the benefit that comes if they are not caught outweighs the risk if they are caught.

In addition, each of us can simply make an error of judgment under the pressure of the situation, and watch it spiral out of control as we helplessly watch from the sidelines, too frightened to take control of the situation.

We professionally encounter many situations in which people who have a problem do things that create a worse problem – آٹا گیلا ہونا غریبی میں – compounding the error of choice. For example, by most standards having an affair or embezzling funds is bad. The consequences of getting caught are worse. However, killing the person who can expose the affair or the embezzlement puts you in an even worse position. By the same token, running someone down while driving – whether drunk or sober – is bad. Fleeing the scene can make the consequences dramatically worse.

One of the factors that cause things to cascade out of control is refusal to acknowledge the cause of the problem, making any proposed solution unrealistic. This is as true for governments as for individuals, although the consequences are more widespread. As an example, one has only to look at Iraq to see how this plays out in real life.

Much of the current discussion is of whether the Iraqis have stepped up to the plate in implementing American-style democracy, and whether we should simply leave if they don't do their part in a timely manner. (Our personal suspicion is that “a timely manner” means somewhere between A) the time it took the U.S. to get from declaring independence from Britain in 1776 until the last battle of the American War of 1812 (in 1815), and B) the time it would take to convert America from civil law to Sharia law.)

However, the assumption that the Iraqis have failed to do their job, after we went in to help them, does not deal with the problem. In truth we went in – with the best of intentions on the part of the average American – under what

proved in retrospect to be the factually false impression on the part of many Americans that Iraq had nuclear and biological weapons. (For a better understanding of weapons of mass destruction in Hussein's Iraq, we recommend the *Comprehensive Report of the Special Advisor to the DCI on Iraq's WMD* of 30 September 2004, which can be found at https://www.cia.gov/cia/reports/iraq_wmd_2004/index.html.) America's subsequent actions have been hindered by the culturally false premise that the 150-plus feuding tribes of Iraq wished to abandon their tribal culture and band together to form an American style democracy. And the politically false premise that the majority of money and talent would not flee the country in time of turmoil. And the sociologically false premise that in times of violence there would be a move toward moderation, rather than the extremism which drove the Christian and Jewish populations from the country, and turned the co-existing Sunni and Shia populations so bitterly against each other, much as we saw in the Balkans.

At the point where the U.S. turns from blaming the Iraqis for not keeping to our timetable on things that are important to us (but seemingly not them), to the actual problems at hand, we will be on our way toward a solution.

Corporations are also guilty of choosing to ignore problems. We see this all too often with products that are discovered to be defective or harmful, where a decision is made not to admit to the problem unless caught. These are too numerous, and too well known, to need to be discussed here.

It is, of course, true that the issue of deliberately ignoring the cause of a problem is only a subset of the larger problem of not having enough information to know the cause of a problem (see the November 2004 issue of **ÆGIS** for an amusing example of this, still with us after 5,000 years). Choosing to deny the root of a problem (as opposed to not understanding it) is, however, an area in which we have some level of control.

The bottom line is that independent of whether you are an individual, a government, or a corporation, you cannot adequately address an issue for which you are responsible if you are unwilling or unable to properly and accurately address its cause. And if you are not willing to take responsibility for the true nature of what is happening, the results are likely to be worse for you than they should be.

4. Technical Issues —Who should investigate your fraud?

The background of a fraud investigator makes a significant difference in the investigation of a fraud. Typically, financial investigators come from one of three backgrounds: Accounting and auditing, law enforcement, and banking or investment banking. All are capable, and each have their strengths.

- Accountants are very good at getting to the heart of the fraud and quantifying the amount of loss.
- Law enforcement is generally good at figuring out what was done wrong and who took advantage of this, at developing a case for prosecution, and at designing a protocol to prevent it from happening again.
- Investment bankers are better at viewing the whole of the fraud, its impact, and appropriate recovery.

Each of these can be important, and the type of fraud and the organizational objectives should play a part in deciding the background of the fraud investigator. It also means that hiring fraud investigators with different backgrounds can bring useful alternatives and choice for the organization.

5. Real Stories from the Field — How dead is dead?

A recent case that went to court ended unsatisfactorily when the defendant died while abroad. The death certificate brought the lawsuit to a close. After the defendant died, we received strong complaints from our client over continuing surveillance for no reason other, in their opinion, than to bill extra hours. They were not happy, to say the least.

Their unhappiness diminished rapidly when the dead defendant made phone calls to one of the people on whom we were conducting the continuing surveillance. Not surprisingly, our client's unhappiness diminished, and that of the judge increased. As, we suspect, will the unhappiness of the deceased once his quickened remains are extradited back to the U.S.

While a death certificate can in many cases be as good as the corpse, not all death certificates are created equal (Editors' note: If you pay more than \$12 for a death certificate in Haiti you are being ripped-off). As a rule of thumb, the more money that is involved in a case, the more we want to see the body and jab it with a pin before we are willing to believe the person is dead.

6. Book and Product Reviews

Awakening Prologue

Centerpointe Research Institute 3 CDs \$159

https://www.centerpointe.com/products/?x=mainnav_index 1-503-672-7117

There is a consensus opinion that meditation is good for you, both physically and mentally. There is also a consensus opinion that it takes a lot of time and practice to be able to develop the ability to train yourself to move your brain waves from beta to alpha to theta to delta.

The folks at Centerpointe Research say they have a way to speed up the process: Their Holosync audio technology allows you to listen to CDs (wearing headphones, since the process depends on differing sounds to each ear) which stimulate the brain, and force it to move to increasingly slower meditative waves.

The beginning program, *Awakening Prologue*, includes a descriptive CD, but the real work starts with the second CD. You first listen to the initial half an hour track once a day. After two weeks you add the second half an hour track. There is a third CD that contains a track designed to put you into an alpha state, which they say makes learning easier, and a track to induce theta waves, which they say increases creativity.

We are not sure how you judge the effectiveness of a product such as this, nor what the exact effects, short or long term, are supposed to be, but we have several friends who swear by these CDs. If you are interested in meditation, or are thinking of trying meditation, *Awakening Prologue* should be of interest to you.

7. Subscription/Unsubscription/Copyright Information

•• **ÆGIS** is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2007 by The **LUBRINCO** Group Ltd, Inc. and Financial Examinations and Evaluations, Inc. It is edited jointly by Richard Isaacs (RBIsaacs@lubrinco.com), L. Burke Files (LBFiles@feeinc.com), and Terry Phillips (TPhillips@aegisjournal.com).

LUBRINCO provides services in three high-threat areas, too specialized to be dealt-with in-house, that can adversely affect domestic and international bottom lines.

- **Identification, valuation, and protection of intellectual assets and critical information.**
 1. American businesses lose \$300 billion annually to competitive intelligence, economic espionage, and information theft.
 2. Sarbanes-Oxley requires internal controls tracking the costs, and impact on valuation, of competitive intelligence, economic espionage, and information theft.
 - LUBRINCO is the leading private sector provider of access to OPSEC, the government-standard process for identification, valuation, and protection of intellectual property and critical information from competitive intelligence, economic espionage, and information theft.
- **International asset location and due diligence.**
 - Location of concealed assets in fraud, theft, and divorce.
 - Due diligence to prevent fraud and loss in China, Central and Eastern Europe, Central Asia, the offshore financial centers, Latin America, and the Caribbean.
 - Financial fraud and anti-money laundering program development and training for compliance with the US *International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001* and the EU *Revised Money Laundering Directive of 2001*.
- **Protection of management, staff, and families.**
 - In the high-threat environments of Latin America, Africa, the Mid-East, and Southeast Asia.
 - When traveling and living overseas.
 - When transporting items of substantial value.

LUBRINCO identifies and quantifies threats and vulnerabilities, and their associated risk, then manages the vulnerabilities so you can transfer or live with the residual risk. We prevent disastrous financial loss to your company, and physical harm to you, your family, and your staff.

For information on **LUBRINCO** and its services, or for the archive of all past issues of **ÆGIS** in PDF format, please go to <http://www.aegisjournal.com/>.

Subscription to **ÆGIS** is available for \$15 per year in North America and \$20 per year outside of North America.

To sign up for a **complimentary subscription** to **ÆGIS** or the **ÆGIS** PDF notification list, go to <http://lb.bcentral.com/ex/manage/subscriberprefs?customerid=7768> or send an email to subscribe@aegisjournal.com.

To subscribe to our AvantGo channel, go to http://avantgo.com/channels/_add_channel.pl?cha_id=1773

To be removed from the subscription list, follow the instructions on the mailing you received, or send an e-mail to unsubscribe@aegisjournal.com.

If you know of anyone else who should be receiving **ÆGIS**, please send their e-mail address to subscribe@aegisjournal.com.

If there is a topic that you would like to know more about, send it to editor@aegisjournal.com and the editors will consider it as the topic for an article in an upcoming issue.

If you would like to submit an article for publication in **ÆGIS**, send it as an attachment to an e-mail to editor@aegisjournal.com. Submission of an article certifies that (a) all information in the article is in the public record, or (b) that you are authorized to release any personal or corporate proprietary information contained in the article, and (c) that none of the article has previously been copyrighted. The submission of materials for publication in **ÆGIS** constitutes a license to **LUBRINCO**, and/or Financial Examinations and Evaluations, Inc, their assigns, associates, or affiliates, to abridge and/or edit said submission, and to copyright and publish/republish any submitted materials in whatever written and/or electronic form they may choose.

If you would like to go beyond normal fair-use in reproducing articles from this issue of **ÆGIS**, you may do so freely as long as appropriate source, copyright, accreditation, and link to the **ÆGIS** Web site is included. This should be in the form

Article Title, from the April 2007 **ÆGIS** (© 2007 **LUBRINCO** & FEEINC), to be found at <http://www.aegisjournal.com/>.

ÆGIS is a forum for the exchange of information, ideas, operating styles,

theories, and related topics for corporate managers who make decisions about threats typically outside the expertise available in-house, yet which have the potential to affect their company's domestic and international bottom lines. Nothing appearing in **ÆGIS** should be construed as legal advice. The information provided is "general information," not "specific advice."

The solution to any problem is highly dependent upon the precise facts involved. Thus, before making any reliance upon anything said here, you should consult with an appropriately skilled professional. Opinions expressed by contributors are not necessarily endorsed by the publisher, and may be presented to encourage a dialogue among subscribers. The publisher and any re-publisher cannot be held responsible for any loss incurred as a result of the application of any information published in **ÆGIS**.

Please be safe, and be smart.